REMARKS

The Office Action dated February 21, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Status of the Claims

Claims 1-21, 27 and 29-37 have been amended to more particularly point out and distinctly claim the subject matter of the invention. New claims 38-51 have been added. Therefore, claims 1-21, 27 and 29-51 are currently pending in the application and are respectfully submitted for consideration.

Improper Finality

On pages 15 and 16 of the Response filed November 8, 2007, Applicant traversed the rejection with respect to independent claims 1, 7, 21, 27 and 29-31, arguing, for example, that "Wright does not disclose or suggest the feature of a user specific record that determines if verification needs to take place". Further, the Applicant traversed the rejections of claims 15 and 35 on pages 17-19 of the Response filed November 8, 2007. However, despite Applicant's clear traversals, the outstanding Office Action failed to address Applicant's arguments. Rather, with respect to claim 1, the outstanding Office Action appears to have substantially copied the arguments presented on pages 4-6 of the Office Action mailed August 23, 2007. The arguments with respect to the other independent claims appear to have been similarly copied. Henry et al. is newly cited in the outstanding Office Action, but was only alleged to disclose that "the specific record is

stored at a server node" (see page 4). With respect to claims 15 and 35, the Office Action also failed to respond to Applicant's arguments. The failure to respond to Applicant's traversals of the rejections presented in the Office Action mailed August 23, 2007, renders the finality of the outstanding Office Action improper.

MPEP § 707.07(f) states that "[i]n order to provide a complete application file history and to enhance the clarity of the prosecution history record, an examiner **must** provide clear explanations of all actions taken by the examiner during prosecution of an application" (emphasis added). "Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it" (*Id.*). "The examiner must address all arguments which have not already been responded to in the statement of the rejection" (MPEP § 707.07(f), Examiner Note 1).

The outstanding Office Action failed to address Applicant's clear traversals. In fact, it does not appear that any of Applicant's arguments are specifically addressed in the outstanding Office Action. Further, failure to specifically respond to Applicant's arguments renders the Office Action arbitrary and capricious, and therefore invalid under the Administrative Procedure Act (5 U.S.C. § 706), a standard to which all Actions by the USPTO must adhere (see *Dickenson v. Zurko*, 527 U.S. 150 (1999)). For at least these reasons, the finality of the outstanding Office Action is improper.

Accordingly, Applicant respectfully requests that the finality of the outstanding Office Action be withdrawn.

Rejections under 35 U.S.C. § 103

Claims 1-14, 16-21, 27, 29-34, 36 and 37 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Chavez et al. (U.S. Patent No. 6,591,102) in view of Wright (U.S. Patent No. 6,957,061) and in further view of Henry et al. (U.S. Patent No. 6,856,800). The Office Action took the position that Chavez et al. discloses all of the features of the independent claims with the exception of "that a specific record contains information that is used to determine that a user is to be verified with a home network" and "that the specific record is stored at a server node" (see, for example, pages 3 and 4). Rather, the Office Action relied on Wright and Henry et al., respectively, to cure these deficiencies of Chavez et al. It is respectfully submitted that the cited art, both individually and in combination, fails to teach or suggest the features of the above-rejected claims. Reconsideration of the claims is respectfully requested.

Independent claim 1, from which claims 2-6 depend, recites a method including using a specific record associated with a user. The specific record is stored at a server node and the specific record contains information that determines that a user characteristic is to be verified with a home network prior to providing access to said service.

Independent claim 7, from which claims 8-20 depend, recites using a user specific record. The user specific record is stored in a server node that indicates a condition that, if satisfied, determines that a user characteristic is to be verified with a home network

prior to providing access to the service. The method also includes providing access to the service in response to the user specific record.

Independent claim 21 recites an apparatus including receiving means for receiving a message from a user terminal, storing means for storing a user specific record associated with the user indicating a condition that, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to a service, and generating means for generating, in response to the user specific record, an access message to provide the user with access to the service from a service provider node.

Independent claim 27 recites an apparatus including record using means for using a user specific record associated with a user indicating a condition that, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to a service. The user specific record is stored in a server node. The apparatus also includes generating means for generating, in response to the user specific record, an access message for providing the user with access to the service from a service provider node.

Independent claim 29 recites a method including storing an authorization and authentication profile associated with a user. The authorization and authentication profile is stored at a serving node in a serving network. The method also includes using the authorization and authentication profile at the serving node. The authorization and authentication profile contains information indicating a condition that, if satisfied,

determines that a user characteristic is to be verified with a home network prior to providing access to the service.

Independent claim 30 recites an apparatus including an interface configured to receive a message from a user terminal and a server node. The server node includes a record using unit configured to use a user specific record associated with the user to indicate a condition that, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to a service. The user specific record is stored in the server node. The server node also includes a generator configured to generate, in response to the user specific record, an access message to provide the user with access to the service from a service provider node.

Independent claim 31 recites an apparatus including a processor and a controller. The controller includes a record using unit configured to use a user specific record associated with a user to indicate a condition that, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to a service. The user specific record is stored in a server node. The apparatus also includes a generator configured to generate, in response to the user specific record, an access message to provide the user with access to the service from a service provider node.

As will be discussed below, the cited art, both individually and in combination, fails to teach or suggest the features of the presently pending claims.

Wright generally discusses:

> a method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of requesting service from a serving network to which the user equipment is not directly subscribed, passing the request for service from the serving network to a home operator network to which the user equipment is directly subscribed, generating an authentication vector in the home operator network which includes an authentication management field, passing the authentication vector from the home operator network to the serving network, passing an authentication element forming at least part of the authentication vector from the serving network to the user equipment, extracting in the user equipment an authentication management field from the authentication element, generating in response at least to a predetermined value of the authentication management field, a predetermined key set identifier, and passing the key set identifier to the serving network.

The parameters of the authentication vector "may be monitored by the user equipment using appropriate timers, accumulators and counters. Before requesting service, the mobile user equipment determines whether the authentication vector should still be valid and issues either the KSI given by the serving network (if no new authentication vector is required) or a special KSI which forces the serving network to request a new authentication vector when the next service request is made" (see column 3, lines 56-67 of Wright).

Claim 1 recites, in part, that "the specific record contains information that determines that a user characteristic is to be verified with a home network prior to providing access to said service." Claims 7, 21, 27 and 29-31, which each have their own scope, recite similar features. The Office Action stated on page 3 that "Chavez fail [sic] to specifically disclose that a specific record contains information that is used to determine that a user is to be verified with a home network." Rather, the Office Action

relied on column 1, lines 25-43 and column 3, lines 56-67 of Wright et al. to allegedly teach these features. Applicant respectfully submits that the cited art, both individually and in combination fails to teach or suggest the features of the above-rejected claims.

Per the above, Wright generally discusses that the mobile user equipment determines whether the authentication vector **should still be valid** before requesting service. The authentication vector can be used "for a predetermined time period, a predetermined number of calls or a predetermined total call duration (which may span more than one call)" (see column 3, lines 56-59). On the other hand, per the above, the independent claims recite that the specific record contains information that determines that a user characteristic **is to be verified** with a home network prior to providing access to said service. In other words, the user characteristic is verified if the information in the specific record indicates that such verification should occur. Wright merely discusses issuing either the KSI given by the serving network (if no new authentication vector is required) or a special KSI which forces the serving network to request a new authentication vector when the next service request is made. Thus, in Wright, it appears that authentication always occurs. Conversely, the independent claims recite performing verification if the specific record contains certain information. Further, nothing is cited or found in Henry et al. that teaches or suggests these features.

Accordingly, it is respectfully submitted that the cited art, both individually and in combination, fails to render the above-mentioned claims obvious under 35 U.S.C. § 103(a).

Claims 2-6, 8-14, 16-20, 32-34, 36 and 37 depend from independent claims 1, 7, 30 or 31 and add further features thereto. Thus, the arguments above with respect to the independent claims also apply to the dependent claims. It is respectfully submitted that the dependent claims patentably distinguish over the cited art for at least the reasons discussed above with respect to the independent claims.

Claims 15 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Chavez et al. in view of Wright and in further view of Basilier et al. (U.S. Patent No. 6,728,536). The Office Action took the position that Chavez et al. and Wright fail to disclose "that the information is specifically requested prior to storing the specific record and is transferred from the AAA-H in response" with respect to claim 15 and "that the information included in the specific record specifically includes a first field for identifying the user and a second field to identify when to authenticate at the AAA-H" with respect to claim 35 (see pages 39 and 40). Rather, the Office Action relied on Basilier et al. to cure these deficiencies of Chavez et al. and Wright. It is respectfully submitted that the cited art, both individually and in combination, fails to teach or suggest the features of the above-rejected claims. Reconsideration of the claims is respectfully requested.

Claim 15 recites that prior to the storing of said user specific record, a request message is generated at a local server node and transmitted to a home authentication, authorization and accounting server of the user. Data comprising the user specific record

is transferred from the home authentication, authorization and accounting server to the local server node in response to the request message.

Claim 35 recites that the user specific record comprises a first data field identifying the user and a second data field determining when authentication or authorization, or both of the user is required in order to access the service.

Basilier et al. generally discusses that "specific information, which may be access specific and/or application specific information is transmitted between visiting and home networks using public IP networks" (column 1, line 67 through column 2, line 3). "In responding to the received registration message, the registration message is sent to the HLR 108 ... [that] generates an appropriate response message which is formatted in the AAA protocol including the AAA protocol encryption" (column 5, lines 11-16 of Basilier et al.). However, with respect to claim 15, nothing is cited or found in Basilier et al. that teaches or suggests that data comprising the user specific record is transferred from the home authentication, authorization and accounting server to the local server node in response to the request message. Rather, a AAA protocol response message is generated - not data comprising a user specific record as claimed.

With respect to claim 35, per the above, Basilier et al. fails to teach or suggest a user specific record. Further, Basilier et al. is silent as to a first data field identifying the user and a second data field determining when at least one of authentication and authorization of the user is required in order to access said service.

Accordingly, it is respectfully submitted that the cited art, both individually and in combination, fails to render the above-mentioned claims obvious under 35 U.S.C. § 103(a).

Further, claims 15 and 35 depend from claims 7 and 30, respectively, and add further features thereto. Nothing is cited or found in Basilier et al. that cures the deficiencies of Chavez et al. and Wright discussed above with respect to the independent claims. Thus, claims 15 and 35 also patentably distinguish over the cited art for at least the reasons discussed above with respect to the independent claims.

New Claims

New claims 38-51 have been added. Claims 42 and 46 are independent method claims, which each have their own scope, that recite similar features to independent apparatus claims 30 and 31, respectively. Claims 50 and 51 are independent software claims, which each have their own scope, that recite similar features to independent apparatus claims 30 and 31, respectively. Claims 38-41, 43-45 and 47-49, which each have their own scope, depend from claims 31, 42 and 46, respectively and are similar to one of claims 32-35. Thus, for at least the reasons argued above, it is respectfully submitted that the new claims also patentably distinguish over the cited art.

Conclusion

As noted previously, claims 1-21, 27 and 29-51 recite subject matter that is neither disclosed nor suggested in the cited art. It is therefore respectfully requested that claims 1-21, 27 and 29-51 be allowed, and this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Michael A. Leonard II
Attorney for Applicant
Registration No. 60,180

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MAL:jf